(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
28. Februar 2002 (28.02.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/17238 A1

(51) Internationale Patentklassifikation[7]: G07C 9/00

(21) Internationales Aktenzeichen: PCT/DE01/02534

(22) Internationales Anmeldedatum:
7. Juli 2001 (07.07.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
PQ 9682 25. August 2000 (25.08.2000) AU

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **ROBERT BOSCH GMBH** [DE/DE]; Postfach 30 02 20, 70442 Stuttgart (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **CROWHURST, Peter** [NZ/AU]; 9 Fernlea Avenue Rowville, Melbourne, VIC 3178 (AU). **PAVATICH, Frank** [AU/AU]; 2 Durban Court, Keilor Downs, Melbourne, VIC 3038 (AU).

(81) Bestimmungsstaaten *(national)*: AU, IN, JP, KR, US.

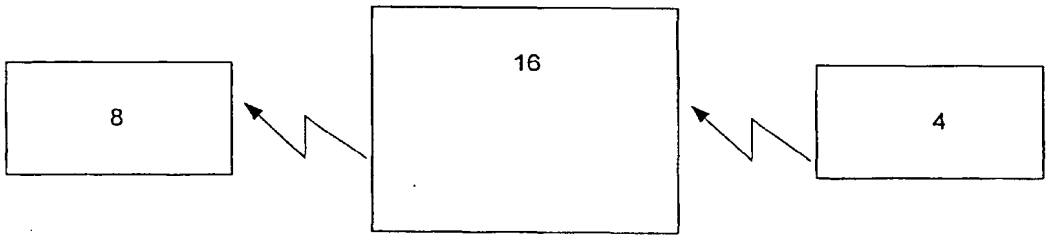
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) **Title:** A SECURITY SYSTEM

(54) **Bezeichnung:** EIN SICHERHEITSSYSTEM



(57) **Abstract:** A security system (4, 8) is disclosed, comprising an electronic key (4) with a transmitter (6) and a secured object with a base station (8) that has a receiver (10). The transmitter (6) and the receiver (10) are so arranged that they communicate with each other for the exchange of authorisation data, whereby the key (4) transmits the data in a message, comprising sections with pre-determined periods (T0, ... T4) with transmission signal variations and the base station (8) recognises distortions in the transmission signal variations by means of a repeater.

(57) **Zusammenfassung:** Es wird ein Sicherheitssystem (4, 8), einschliesslich einem elektronischen Schlüssel (4), der einen Sender (6) aufweist, und einem gesicherten Objekt mit einer Basisstation (8), die einen Empfänger (10) aufweist, wobei der Sender (6) und der Empfänger (10) so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, vorgeschlagen, wobei der Schlüssel (4) die Daten in einer Nachricht übermittelt, die Teile mit jeweils vorherbestimmten Perioden (T0, ... T4) mit Übertragungssignalvariationen umfasst, und wobei die Basisstation (8) Verzerrungen der Übertragungssignalvariationen durch eine Relaisstelle erkennt.

WO 02/17238 A1

EIN SICHERHEITSSYSTEM

Die vorliegende Erfindung bezieht sich auf ein Sicherheitsssystem, insbesondere ein passives Sicherheitssystem für Fahrzeuge.

Derzeit existierende passive Fahrzeug-Sicherheitssysteme für den Zugang oder die Inbetriebsetzung von Fahrzeugen verwenden fernbetätigte elektronische Schlüssel, die einen Sender einschließen, der Authentifizierungsdaten an einen in dem Fahrzeug befindlichen Empfänger übermittelt, wenn ein Transponder eines Schlüssels erregt wird, wenn der Schlüssel innerhalb eines vorbestimmten Bereichs des Empfängers ist. Das zwischen dem Sender und dem Empfänger aktivierte Kommunikationsprotokoll benutzt eine Radiofrequenz-Schnittstelle zum Führen der übertragenen Daten sowie aller Daten, die von dem Fahrzeug an den Schlüssel gesandt werden. Die Radiofrequenz (RF)-Schnittstelle hat einen begrenzten Bereich, um zu gewährleisten, daß die Kommunikationsverbindung unterbrochen wird, wenn sich eine im Besitz des Schlüssels befindliche Person aus der unmittelbaren Nähe des Fahrzeugs entfernt.

Passive Sicherheitssysteme sind leicht Angriffen unbefugter Personen ausgesetzt, die Intercept-Einrichtungen benutzen, die in die Nähe des Fahrzeugs und des Schlüssels gebracht werden. Die Einrichtung wird benutzt, um den Schlüssel zu erregen, die von dem Schlüssel übermittelten Übertragungen zu empfangen und die Übertragungen an das Fahrzeug weiterzuübertragen. Die Intercept-Einrichtung, die vielfach als Relaisstelle bezeichnet wird, umfaßt normerweise einen Empfänger und einen Verstärker innerhalb des Bereichs des Schlüssels, um das abgefangene Signal an einen Empfänger und einen Verstärker in der Nähe des Fahrzeugs zu übertragen, um Zugang zu dem Fahrzeug zu erhalten.

Die Spezifikationen der australischen Patentanmeldungen 33933/99 und 42419/99, nachstehend als "die Zweiton-Sicherheitssystem-Spezifikationen" bezeichnet und durch Bezugnahme in diese Beschreibung einbezogen, beschreiben Sicherheitssysteme, die benutzt werden können, um Angriffe seitens Relaisstellen zu verhindern oder zu erkennen, wenn die Relaisstelle einen Breitbandverstärker benutzt, um Signale abzufangen, die zwischen dem Schlüssel und dem Fahrzeug übertragen werden, wobei eine Anzahl von verschiedenen RF - Übertragungskanälen benutzt werden. Die Relaisstelle kann entdeckt werden, wenn ein Zweitontest, wie in den zwei Zweiton-Sicherheitssystem-Spezifikationen beschrieben, verwendet wird.

Es ist jedoch möglich, daß eine Relaisstelle Einrichtungen verwendet, die keinen Breitbandverstärker einbeziehen, sondern sich stattdessen separater Empfänger, Filter und Verstärker für jeden Übertragungskanal bedienen. Die Relaisstelle kann separate Sender/Empfängerstationen haben, die jeweils mit einem Empfänger und Sender ausgerüstet sind, der auf jeden Radiofrequenzkanal in dem Frequenzband, in welchem das passive Sicherheitssystem betrieben wird, dediziert ist. Die Relaisstelle würde dann das Frequenzband des Sicherheitssystems nicht abzutasten brauchen, um die Kanäle zu lokalisieren, die beide für die spektrale Authentifizierung der Daten und Transponder verwendet werden. In diesem Szenario kann der Zweitontest nicht zur Erkennung angewendet werden, um die von dem abfangenden Breitbandverstärker beim Mischen der Übertragungskanäle erzeugte Seitenbandintermodulation zu erkennen. Demgemäß ist es wünschenswert, ein Sicherheitssystem bereitzustellen, welches zur Verhinderung dieser Art Angriff oder zumindest als eine zweckmäßige Alternative zum Einsatz kommen kann.

Die vorliegende Erfindung stellt ein Sicherheitssystem vor, einschließlich einem elektronischen Schlüssel, der einen Sender aufweist, und einem gesicherten Gegenstand mit einer Basisstation, die einen Empfänger aufweist, wobei der Sender und der Empfänger so ausgelegt sind, daß sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, dadurch gekennzeichnet, daß

der Schlüssel, der die Daten in einer Nachricht übermittelt, Teile mit jeweils vorherbestimmten Perioden mit Übertragungssignalvariationen umfaßt; und

daß die Basisstation Verzerrungen der Übertragungssignalvariationen durch eine Relaisstelle erkennt.

Die vorliegende Erfindung stellt auch eine Kommunikationsmethode vor, die von einem Sicherheitssystem durchgeführt wird, einschließlich einem elektronischen Schlüssel, der einen Sender aufweist, und einem gesicherten Objekt mit einer Basisstation, die einen Empfänger aufweist, wobei die Methode die Übermittlung von Authentifizierungsdaten von dem Sender an den Empfänger umfaßt, charakterisiert durch

Übermittlung der Daten in einer Nachricht, welche Teile mit jeweils vorherbestimmten Perioden mit Übertragungssignalvariationen umfaßt; und

Erkennung an der Basisstation von Verzerrungen der Übertragungssignalvariationen durch eine Relaisstelle.

Eine bevorzugte Realisierung der vorliegenden Erfindung ist nur beispielsweise nachfolgend mit Bezug auf die beiliegenden Zeichnungen beschrieben:

Figur 1 ist eine schematische Darstellung einer bevorzugten Realisierung eines Sicherheitssystems mit einer Relaisstelle;
Figur 2 ist ein Blockdiagramm eines Sicherheitssystems;
Figur 3 ist ein Zeitdiagramm für von dem Sicherheitssystem übermittelte Signale;
Figur 4 ist ein Diagramm eines verfälschten Datensignals;
Figur 5 ist ein Diagramm eines Frequenzspektrums für Zweiton-Übertragung des Systems; und
Figur 6 ist ein Diagramm eines Frequenzspektrums für Datenübermittlung des Systems.

Ein passives Sicherheitssystem, wie in Figuren 1 und 2 gezeigt, umfaßt einen elektronischen Schlüssel 4 mit einem Sender 6 und einer Sendeantenne 7, einer Basisstation 8 mit einem Empfänger 10 und Empfangsantenne 12. Die Basisstation 8 ist an einem gesicherten Ort untergebracht, wie z.B. einem Fahrzeug, und kontrolliert den Zugang zu dem gesicherten Ort

und/oder zum Starten des Fahrzeugs. Wenn der Schlüssel 4 innerhalb eines bestimmten Bereichs der Antenne 12 des Empfängers 10 herangeführt wird, erregt der Empfänger 10 den Transponder des Schlüssels 4, und veranlaßt dadurch den Sender 6, die Übermittlung an den Empfänger 10 zu beginnen. Daten werden unter Verwendung von RF-Signalen übermittelt, welche eine Kommunikationsverbindung zwischen dem Schlüssel 4 und der Basisstation 8 herstellen. Die zwischen dem Schlüssel 4 und der Basisstation 8 übermittelten Daten werden durch ein Kommunikationsprotokoll bestimmt, welches der Schlüssel 4 und die Basisstation 8 befolgen, und welches die Übermittlung von Authentifizierungsdaten von dem Schlüssel 4 an den Empfänger 10 beinhaltet. Zugang zu dem gesicherten Bereich und/oder zum Starten des Fahrzeugs wird von der Basisstation 8 nur dann zugelassen, wenn die übermittelten Authentifizierungsdaten mit den von der Basisstation 8 gespeicherten Authentifizierungsdaten übereinstimmen.

Der Schlüssel 4 und die Basisstation 8 umfassen eine Reihe von Sicherheitsmerkmalen, wie z.B. diejenigen, die in den Zweiton-Sicherheitssystem-Spezifikationen beschrieben sind. Die Bauteile des Schlüssels 4 und der Basisstation 8 sind dieselben wie in den Zweiton-Sicherheitssystem-Spezifikationen beschrieben, mit der Ausnahme, daß der Sender 6 des Schlüssels 4 und der Empfänger 10 der Basisstation 8 zusätzliche Filter mit größeren Bandbreiten, wie unten beschrieben, einschließen oder programmierbare Filter, deren Bandbreiten angeglichen werden können. Auch die Steuer-Software in dem Schlüssel 4 und der Basisstation 8 wird angeglichen, so daß das Kommunikationsprotokoll, wie unten in Bezug auf Figur 3 beschrieben, ausgeführt wird.

Der Schlüssel 4 schließt einen Mikrocontroller 35 ein, der Steuer-Software zur Steuerung der Schlüsselkomponenten als Teil des Kommunikationsprotokolls umfaßt. Der Mikrocontroller 35 steuert den Sender 6, welcher einen ersten Oszillator 30 zur Erzeugung des ersten Grundtons 60 und einen zweiten Oszillator 32 zur Erzeugung des zweiten Grundtons 62 einschließt. Die erzeugten Frequenzsignale werden von einem Kombinator (Antennenweiche) oder Summierverstärker 34 für Übertragung auf der UHF Sendeantenne 7 kombiniert. Der Mikrocontroller 35 ist auch zur Steuerung der Oszillatoren 30 und 32 angeschlossen, so daß er

einen Frequenzversatz oder eine Frequenzabweichung, gestützt auf die zu übertragenden Daten, wie nachstehend beschrieben, bewirken kann. Der Mikrocontroller 35 ist auch befähigt, Steuerdaten von der Basisstation 8 über einen Niederfrequenz-Empfänger 9 und Antenne 31 zu empfangen. Der Schlüssel 4 schließt eine Transponderschaltungsanordnung (nicht dargestellt) ein, um den Schlüssel 4 zu erregen oder zu triggern, wenn er innerhalb eines vorbestimmten Bereichs der Basisstation 8 ist. Innerhalb dieses Bereichs kann ein Erregungssignal seitens des Fahrzeugs erzeugt werden, wenn ein bestimmtes Ereignis eintritt, wie z.B. das Anheben des Türgriffes oder ähnliches. Sobald der Schlüssel 4 erregt oder aktiviert ist, wird das Kommunikationsprotokoll 4 für die Zugriffsberechtigung des Fahrzeugs in Gang gesetzt.

Die Basisstation 8 umfaßt einen Mikrocontroller 40, der Steuer-Software aufweist und welcher den Betrieb der Komponenten der Basisstation 8 steuert. Diese Teile umfassen einen UHF-Empfänger 36, der mit der Empfangsantenne 12 verbunden ist, um eine Ausgabe der für den Mikrocontroller 40 empfangenen Daten bereitzustellen.
Ein Analog/Digital-Umsetzer 38 wird verwendet, um analoge Ausgangssignale des Empfängers 36 in digitale Form für den Mikrocontroller 40 umzusetzen. Diese Signale schließen eine RSSI (Eingangssignalstärkenanzeiger)- Ausgabe ein, welche spektrale Signaturdaten für den Mikrocontroller 40 bereitstellt. Zwischenfrequenzsignale, die von dem Empfänger 36 erzeugt werden, werden an Filter 43 zum Filtern weitergeleitet und dann an den Empfänger 36 zurückgeleitet, um die von den Signalen geführten Daten auszublenden. Die Filter 43 sind geschaltete ("switched") Zwischenfrequenzfilter mit Bandbreiten, die von dem Mikrocontroller 40 in Übereinstimmung mit dem Protokoll eingestellt werden. Die Basisstation 8 hat auch einen Niederfrequenzsender 37 und Antenne 39 zur Übertragung von Daten von dem Mikrocontroller 40 an den Schlüssel 4. Der Niederfrequenzsender 37, Antennen 31 und 39 und Empfänger 9 des Schlüssels 4 sind so ausgelegt, daß eine Niederfrequenz-Kommunikationsverbindung nur dann hergestellt wird, wenn der Schlüssel 4 und die Basisstation 8 gemeinsam innerhalb des gesicherten Bereichs untergebracht sind, z.B. innerhalb des Fahrzeugs. Zum Beispiel kann die Sendeantenne 39 in Form einer Spule sein, die in dem Zündsystem (ignition barrel) 39 untergebracht ist, so daß

eine Verbindung nur dann mit der Antenne 31 hergestellt wird, wenn der Schlüssel 4 in den Zündschalter des Zündsystems eingeführt wird. Die Niederfrequenzkanal-Verbindung wird benutzt, um Synchronisationskontrolldaten von der Basisstation an den Schlüssel 4 zu senden zur Verwendung wenn der Schlüssel 4 das nächste Mal erregt wird. Die Synchronisationskontrolldaten werden dazu benutzt, die Zeiten T0, T1, T2, T3 und T4 für die verschiedenen Teile oder Komponenten der in dem Zugriffsberechtigungsprotokoll übersandten Nachrichten einzustellen.

Das in Figur 3 dargestellte Protokoll, beginnend bei Stufen (a) und (b) beinhaltet die zwei von dem Schlüssel 4 übermittelten Grundtöne mit 100 kHz Abstand, zuerst bei geringer Leistung und dann bei hoher Leistung, und Durchführung des Zweitontests, wie in den Zweiton-Sicherheitssystem-Spezifikationen beschrieben. Ein Beispiel des Frequenzspektrums der von dem Empfänger 10 während zwei Tonübertragungen empfangenen Signale ist in Figur 5 dargestellt. Falls, zum Beispiel, die Grundton-Oszillatoren 30 und 32 dafür eingestellt sind, 433,9 MHz bzw. 434,1 MHz zu übertragen, dann werden alle Intermodulationsverzerrungsprodukte "dritter Ordnung" (third order) bei den Frequenzen 433,7 MHz und 434,3 MHz, 64 bzw. 66, erscheinen. Der Mikrocontroller 40 stellt die Filter 43 so ein, daß entsprechende Bandbreitenfilter von 100 kHz Breite für jede der Frequenzen 60, 62, 64 und 66 bereitgestellt werden. Die spektrale Information innerhalb dieser Bänder wird in eine Spektralsignatur für den Mikrocontroller 40 umgesetzt und mit gespeicherter Spektralmaske verglichen, um Störung einer jeden Relaisstelle 16 gemäß dem Zweitontest zu erkennen.

Die Fähigkeit, eine Relaisstelle mittels des Zweitontests zu erkennen, wird durch das synchronisierte Schalten der Niederleistungs- und der Hochleistungs-Übertragungsteile (a) und (b) der übermittelten Nachricht maximiert. Die von einer Relaisstation 16 in die Intermodulationsbänder eingeführten Verzerrungsprodukte vermehren sich dreifach für jede einzelne Leistungserhöhung. Während des Anfangsübertragungsteils (a) in geringer Leistung, müßte eine Relaisstelle 16 ihren Verstärkern eine beträchtliche Leistungsverstärkung oder einen beträchtlichen Leistungsgewinn zuführen, um den Abstand zwischen dem Schlüssel 4

und der Basisstation 8 des Fahrzeugs zu überbrücken. Wenn der Schlüssel 4 beginnt, die Hochleistungskomponente (b) durch Steigerung des Leistungsgewinns der Verstärker 34 bei einer Synchronisationszeit zu übertragen, die von der Basisstation 8 vorgeschrieben wird, ist die Relaisstelle 16 nicht in der Lage, den Leistungsgewinn seiner Verstärker sofort auszugleichen, und wird ein übertrieben verstärktes Signal an den Empfänger 10 übertragen. Falls zum Beispiel der Schlüssel 4 eine Leistungserhöhung von 30 dB am Ende der Periode T0 einführt, dann werden sich die Verzerrungsprodukte in den Intermodulationsbändern um 90 dB erhöhen. Dadurch wird gewährleistet, daß in unvorteilhaften Umständen, wenn ansonsten die Intermodulationsprodukte innerhalb des Rauschpegels (noise floor) des Empfängers 10 wären, diese Produkte zu einem Leistungspegel angehoben würden um sicherzustellen, daß sie innerhalb der Meßfähigkeit des Empfängers 10 sind.

Bei Stufe (c) werden die zwischen der Basisstation und dem Schlüssel zu übertragenden Authentifizierungsdaten in einem ersten Teil gesandt. Sie werden jedoch gesandt unter Verwendung von Frequenzumschaltung (frequency shift keying) und Anlegen einer Frequenzabweichung, z.B. 200 kHz, von dem gewählten Übertragungskanal. In anderen Worten, wird ein niedriges Signal 70 wird mit einer +200 kHzAbweichung gesandt, und ein höheres Signal 72 wird mit einer -200 kHZ·Abweichung gesandt. Das Frequenzspektrum der von dem Empfänger 10 während der fsk-Datenübertragung empfangenen Signale ist in Figur 6 dargestellt. Da die Filter 43 des Empfängers 10 vorher auf eine Bandbreite von 100 kHz eingestellt worden sind, müssen sie abgeglichen werden, um Datenverfälschung zu vermeiden. Dementsprechend wird während einer Anfangsübertragung, wie z.B. vor oder während des Zweitontests, der Schlüssel von der Basisstation angewiesen, eine bestimmte Anzahl von Bits bei einer gesetzten Frequenzabweichung nach den Stufen (a) und (b) zu übertragen. Dementsprechend wird der Filterkreis 43 in dem Empfänger 10 geändert, um die erforderliche neue Bandbreite von 400 kHz zur richtigen Zeit bedienen zu können. Die Anzahl der zu übertragenden Bits und Frequenzabweichungen können an den Schlüssel übersandt werden unter Verwendung einer Anfangsnachricht, die durch Erkennung und Gültigkeitsprüfung des Schlüssels seitens der Basisstation ausgelöst wird. Diese Anfangsnachricht wird verschlüsselt und unter Benutzung der Niederfrequenzverbindung gesandt. Der Zeitablauf der

Kommunikation ist so ausgelegt, daß die Relaisstelle unfähig ist, Filter zur richtigen Zeit anzugleichen oder zu ändern. Wenn daher die Daten mit der breiteren Frequenzabweichung gesandt werden, kann das Abfangen durch eine Relaisstelle, die schmale Bandbreiten-Filter 100 kHz benutzt, um den Zweitontest zu umgehen, an der Basisstation 8 erkannt werden, da Benutzung der schmalen Bandbreitenfilter eine Datenverfälschung, wie in Figur 4 gezeigt, einführen würde. Die in Figur 4 dargestellte Verfälschung wird durch einen 150 kHz Bandbreitenfilter eingeführt, wenn eine Frequenzabweichung von +/- 150 kHz auf die übertragenen Daten angewendet wird.

Bei Stufe (d) werden die zwei Grundtöne wiederum mit 100 kHz Kanalabstand übertragen. Der Grund ist der, wiederum den Zweitontest durchzuführen, um zu erkennen, ob die Relaisstelle nun die Bandbreite irgendeines an der Relaisstelle benutzten Zwischenfrequenzfilters (IF) erweitert hat. Falls zum Beispiel die Bandbreite nun auf 400 kHz erhöht worden ist, wird der Zweitontest, der an dieser Stufe benutzt wird, in der Lage sein, die Anwesenheit des breiteren Bandbreitenfilters zu erkennen, da sich dadurch ein Mischen der Töne und der erkennbaren Intermodulation ergeben wird. Die Dauer 73 der während dieser Nachricht versandten Töne wird wiederum während der Anfangsnachricht an den Schlüssel 4 mitgeteilt. Dies wird wiederum verhindern, daß die Relaisstelle die Filter zur richtigen Zeit während des Kommunikationsprotokolls angleicht.

Bei Stufe (e) wird der zweite Teil der Authentifizierungsdaten bei einer Frequenzabweichung von +/- 200 kHz überwiesen. Dies wiederum wurde vorher von der Basisstation an den Schlüssel mitgeteilt, damit die Sicherheitssystemfilter entsprechend angeglichen oder geschaltet werden können.

Die Zeitabläufe für jeden der Teile der von dem Schlüssel 4 übertragenen Nachricht, T0, T1, T2, T3 und T4, und gegebenenfalls der zur Übertragung der Daten in den Datenteilen (c) und (e) benutzten Frequenzabweichungen werden von der Basisstation nach jeder gültigen Erkennung des Schlüssels 4 geändert. Diese Zeitablaufs- oder Synchronisationsdaten werden dem Schlüssel 4 mit der Anfangsnachricht zugeführt; Teile der Anfangsnachricht können, wie

vorstehend beschrieben, während der Übertragung von Teilen der Nachricht durch den Schlüssel übertragen werden, werden aber bevorzugterweise übersandt, wenn der Schlüssel 4 und die Basisstation 8 gemeinsam innerhalb des gesicherten Bereichs untergebracht sind, z.B. nachdem das Fahrzeug gestartet worden ist. Die neuen Synchronisationszeiten und Abweichungen werden dann für die nächste Kommunikation über die RF Schnittstelle verwendet. Man bedient sich hierbei der Zufallsauswahl (random selection) um zu vermeiden, daß die Relaisstelle 16 die Zeitabläufe und Abweichungen lernt. Die Frequenzabweichungen zur Übertragung der hohen und niedrigen Bits der Daten kann gemäß den Fähigkeiten des eingesetzten Senders 6 und Empfängers 10 variiert werden. Zum Beispiel kann die Abweichung so gering wie z.B. +/- 25 kHz sein. Die Bandbreite des von dem Empfänger 10 benutzten Filters und die angewandte Abweichung braucht einfach nur während der Übertragung der Schlüsselnachricht geändert werden, um die Anwesenheit von Filtern zu erkennen, die von einer Relaisstelle 16 benutzt werden. Falls die Frequenzabweichung während der Übertragung der Datenteile über die Bandbreite des Filters einer Relaisstelle 16 hinausgeht, dann werden die Daten von der Relaisstelle 16 verfälscht und von der Basisstation 8 erkannt. Falls die Filter der Relaisstelle breit genug sind, daß die Daten nicht verfälscht werden, dann werden die zwei Töne von den Filtern durchgelassen und die erkennbaren Intermodulationsprodukte werden erzeugt. Auch wenn die Relaisstelle genügend durchgebildet ist, um Zwischenfrequenzfilter zu schalten, um die Änderung in der Bandbreite auszugleichen, ist die Relaisstelle 16 unfähig festzustellen, wann die Filterbandbreite geändert werden müßte. Um Erfolg zu haben, würde die Relaisstelle die Filterbandbreiten genau zum richtigen Zeitpunkt ändern müssen, sonst wird der Zweitontest ihre Anwesenheit aufdecken oder aber die Daten werden verfälscht.

Das Protokoll kann abhängig von den Sicherheitserfordernissen für den gesicherten Bereich variiert werden. Zum Beispiel kann auf die Leistungsvariation zwischen den Teilen (a) und (b) verzichtet werden und einfach nur ein Zweitontest einheitlicher Leistung angewendet werden. Es kann auch vielleicht die Entscheidung getroffen werden, daß die Unterteilung der Authentifizierungsdaten in zwei Teile nicht erforderlich ist, und daß alle Daten in der Periode anschließend an die ersten Zweitontests gesandt werden, wodurch sich die Notwendigkeit für

Teil (d) erübrigt. Falls die Daten in einen Teil kombiniert werden, können sie mit den Niederleistungs- und Hochleistungs- Zweitontest-Teilen gesandt werden oder dem Zweitontest der einzelnen einheitlichen Leistung.

Synchronisierung erfolgt von dem Punkt an, wo der Schlüssel 4 erregt ist und gültige Kommunikation mit der Basisstation 8 einleitet. Diese gültige Kommunikation kann durch den Benutzer des Schlüssels, wie zuvor beschrieben, eingeleitet werden.

Dem Fachkundigen werden hierzu eine Vielzahl von Abwandlungen gegenwärtig werden, ohne daß der Umfang der vorliegenden Erfindung, wie sie hiermit unter Bezug auf die beiliegenden Zeichnungen beschrieben wird, überschritten wird.

Patentansprüche

1. Ein Sicherheitssystem (4,8), einschließlich einem elektronischen Schlüssel (4), der einen Sender (6) aufweist, und einem gesicherten Objekt mit einer Basisstation (8), die einen Empfänger (10) aufweist, wobei der Sender (6) und der Empfänger (10) so ausgelegt sind, daß sie miteinander kommunizieren, um Authentifizierungsdaten auszutauschen, dadurch gekennzeichnet, daß
der Schlüssel (4), die Daten in einer Nachricht übermittelt, die Teile mit jeweils vorherbestimmten Perioden (T0,... T4) mit Übertragungssignalvariationen umfaßt; und daß
die Basisstation (8) Verzerrungen der Übertragungssignalvariationen durch eine Relaisstelle erkennt.
2. Ein Sicherheitssystem nach Anspruch 1, wobei mindestens einer der Teile dieser Nachricht Daten mit einer Frequenzabweichung von einer Übertragungskanalfrequenz überträgt, um Verfälschung der Daten durch einen Filter einer Relaisstelle zu erkennen.
3. Ein Sicherheitssystem nach Anspruch 2, wobei die Frequenzabweichung zusammen mit der Bandbreite des Filterkreises abgeglichen wird.
4. Ein Sicherheitssystem nach Anspruch 1, wobei ein Filterkreis (43) des Empfängers (10) von der Basisstation (8) gesteuert wird, um synchron die Übertragungssignalvariationen für die vorherbestimmten Perioden abzugleichen.
5. Ein Sicherheitssystem nach Anspruch 4, wobei die Nachricht einen ersten Teil mit einer ersten Periode aufweist und der Filterkreis eine erste Bandbreiteneinstellung für die erste Periode hat;
die Nachricht einen zweiten Teil mit einer zweiten Periode aufweist, um mindestens einen Teil der Daten mit einer Frequenzabweichung von einer Übertragungskanalfrequenz zu übertragen und der Filterkreis eine zweite Bandbreiteneinstellung für die zweite Periode benutzt; und
die Basisstation Verfälschung der Daten durch einen Filter der Relaisstelle erkennt.
6. Ein Sicherheitsystem nach Anspruch 5, wobei eine Anzahl des zweiten Teils, durchschossen von dem ersten Teil, benutzt wird, um die Daten zu übertragen.

7. Ein Sicherheitssystem nach Anspruch 5, wobei die erste Bandbreiteneinstellung eine Bandbreite hat, die schmaler ist als die Bandbreite der Frequenzabweichung der zweiten Bandbreiteneinstellung.

8. Ein Sicherheitssystem nach Anspruch 7, wobei die erste Bandbreiteneinstellung jeweils erste Bandbreiten für zwei Töne und Intermodulationsprodukte der Töne hat, und die Basisstation einen Spektralsignaturtest an in den Bandbreiten empfangenen Signalen durchführt, um eine Relaisstelle zu erkennen.

9. Ein Sicherheitssystem nach Anspruch 8, wobei die erste Periode eine Anfangsperiode mit einer ersten Übertragungssignalleistung und eine nachfolgende Periode mit einer zweiten Übertragungssignalleistung einschließt, die verschieden von der ersten Leistung ist.

10. Ein Sicherheitssystem nach Anspruch 8, wobei eine Anzahl des zweiten Teils, durchschossen von einem ersten Teil, benutzt wird, um die Daten zu übertragen.

11. Ein Sicherheitssystem nach Anspruch 9, wobei eine Anzahl des zweiten Teils, durchschossen von einem ersten Teil, benutzt wird, um die Daten zu übertragen.

12. Ein Sicherheitssystem nach Anspruch 11, wobei nur der erste (der Anfang) des ersten Teils die Anfangsperiode und die nachfolgende Periode einschließt.

13. Ein Sicherheitssystem nach Anspruch 1, wobei die Nachricht einen ersten Teil mit einer ersten Periode aufweist und der Filterkreis eine erste Bandbreiteneinstellung für die erste Periode benutzt und die erste Periode eine Anfangsperiode mit einer ersten Übertragungssignalleistung einschließt und eine nachfolgende Periode mit einer zweiten Übertragungssignalleistung, die verschieden von der ersten Leistung ist.

14. Ein Sicherheitssystem nach Anspruch 13, wobei die Nachricht einen ersten Teil mit einer ersten Periode hat und der Filterkreis eine erste Bandbreiteneinstellung für die erste Periode benutzt und die erste Bandbreiteneinstellung jeweils erste Bandbreiten für zwei Töne und Intermodulationsprodukte der Töne aufweist, und die Basisstation einen Spektralsignaturtest an in den Bandbreiten empfangenen Signalen durchführt, um eine Relaisstelle zu erkennen.

15. Ein Sicherheitssystem nach einem der Ansprüche 1 bis 14, wobei die Perioden von der Basisstation eingestellt werden und an den Schlüssel kommuniziert werden.

16. Ein Sicherheitssystem nach Anspruch 15, wobei die Perioden mittels Zufallsauswahl (random selection) bestimmt werden.

17. Ein Sicherheitssystem nach Anspruch 15, wobei die Perioden geändert und kommuniziert werden, wenn der Schlüssel als gültig befunden worden ist.

18. Ein Sicherheitssystem nach Anspruch 15 oder 17, wobei die Perioden kommuniziert werden, wenn der Schlüssel sich in dem gesicherten Objekt befindet.

19. Ein Fahrzeug mit einem Sicherheitssystem nach einem beliebigen der Ansprüche 1 bis 18.

20. Eine Kommunikationsmethode, die von einem Sicherheitssystem durchgeführt wird, einschließlich einem elektronischen Schlüssel (4), der einen Sender (6) aufweist, und einem gesicherten Objekt mit einer Basisstation (8), die einen Empfänger (10) aufweist, wobei die Methode die Übermittlung von Authentifizierungsdaten von dem Sender (6) an den Empfänger (10) umfaßt, charakterisiert durch
Übermittlung der Daten in einer Nachricht, welche Teile mit jeweils vorherbestimmten Perioden mit Übertragungssignalvariationen umfaßt;
und Erkennung an der Basisstation (8) von Verzerrungen der Übertragungssignalvariationen durch eine Relaisstelle.

21. Eine Kommunikationsmethode nach Anspruch 20, wobei mindestens einer der Teile dieser Nachricht Daten mit einer Frequenzabweichung von einer Übertragungskanalfrequenz überträgt, um Verfälschung der Daten durch einen Filter einer Relaisstelle zu erkennen.

22. Eine Kommunikationsmethode nach Anspruch 21, wobei die Frequenzabweichung zusammen mit der Bandbreite des Filterkreises abgeglichen wird.

23. Eine Kommunkationsmethode nach Anspruch 20, wobei ein Filterkreis (43) des Empfängers (10) gesteuert wird, um synchron die Übertragungssignalvariationen für die vorherbestimmten Perioden abzugleichen.

24. Eine Kommunikationsmethode nach Anspruch 23, wobei die Nachricht einen ersten Teil mit einer ersten Periode aufweist und der Filterkreis eine erste Bandbreiteneinstellung für die erste Periode hat;
die Nachricht einen zweiten Teil mit einer zweiten Periode aufweist, um mindestens

einen Teil der Daten mit einer Frequenzabweichung von einer Übertragungskanalfrequenz zu übertragen und der Filterkreis eine zweite Bandbreiteneinstellung für die zweite Periode benutzt; und die Basisstation Verfälschung der Daten durch einen Filter der Relaisstelle erkennt.

25. Eine Kommunikationsmethode nach Anspruch 24, wobei eine Anzahl des zweiten Teils, durchschossen von dem ersten Teil, benutzt wird, um die Daten zu übertragen.

26. Eine Kommunkationsmethode nach Anspruch 24, wobei die erste Bandbreiteneinstellung eine Bandbreite hat, die schmaler ist als eine Bandbreite der Frequenzabweichung der zweiten Bandbreiteneinstellung.

27. Eine Kommunikationsmethode nach Anspruch 26, wobei die erste Bandbreiteneinstellung jeweils erste Bandbreiten für zwei Töne und Intermodulationsprodukte der Töne hat, und die Basisstation einen Spektralsignaturtest an in den Bandbreiten empfangenen Signalen durchführt, um eine Relaisstelle zu erkennen.

28. Eine Kommunikationsmethode nach Anspruch 27, wobei die erste Periode eine Anfangsperiode mit einer ersten Übertragungssignalleistung und eine nachfolgende Periode mit einer zweiten Übertragungssignalleistung einschließt, die verschieden von der ersten Leistung ist.

29. Eine Kommunikationsmethode nach Anspruch 27, wobei eine Anzahl des zweiten Teils, durchschossen von einem ersten Teil, benutzt wird, um die Daten zu übertragen.

30. Eine Kommunikationsmethode nach Anspruch 28, wobei eine Anzahl des zweiten Teils, durchschossen von einem ersten Teil, benutzt wird, um die Daten zu übertragen.

31. Eine Kommunikationsmethode nach Anspruch 30, wobei nur der erste (der Anfang) des ersten Teils die Anfangsperiode und die nachfolgende Periode einschließt.

32. Ein Kommunikationsmethode nach Anspruch 20, wobei die Nachricht einen ersten Teil mit einer ersten Periode aufweist und der Filterkreis eine erste Bandbreiteneinstellung für die erste Periode benutzt und die erste Periode eine Anfangsperiode mit einer ersten Übertragungssignalleistung einschließt und eine nachfolgende Periode mit einer zweiten Übertragungssignalleistung, die verschieden von der ersten Leistung ist.

33. Eine Kommunikationsmethode nach Anspruch 32, wobei die Nachricht einen ersten Teil mit einer ersten Periode hat und der Filterkreis eine erste Bandbreiteneinstellung für die erste Periode benutzt und die erste Bandbreiteneinstellung jeweils erste Bandbreiten für zwei Töne und Intermodulationsprodukte der Töne aufweist, und die Basisstation einen Spektralsignaturtest an in den Bandbreiten empfangenen Signalen durchführt, um eine Relaisstelle zu erkennen.

34. Eine Kommunikationsmethode nach einem der Ansprüche 20 bis 33, wobei die Perioden von der Basisstation eingestellt werden und an den Schlüssel kommuniziert werden.

35. Eine Kommunikationsmethode nach Anspruch 34, wobei die Perioden mittels Zufallsauswahl (random selection) bestimmt werden.

36. Eine Kommunikationsmethode nach Anspruch 34, wobei die Perioden geändert und kommuniziert werden, wenn der Schlüssel als gültig befunden worden ist.

37. Ein Kommunikationsmethode nach Anspruch 34 oder 36, wobei die Perioden kommuniziert werden, wenn der Schlüssel sich in dem gesicherten Objekt befindet.

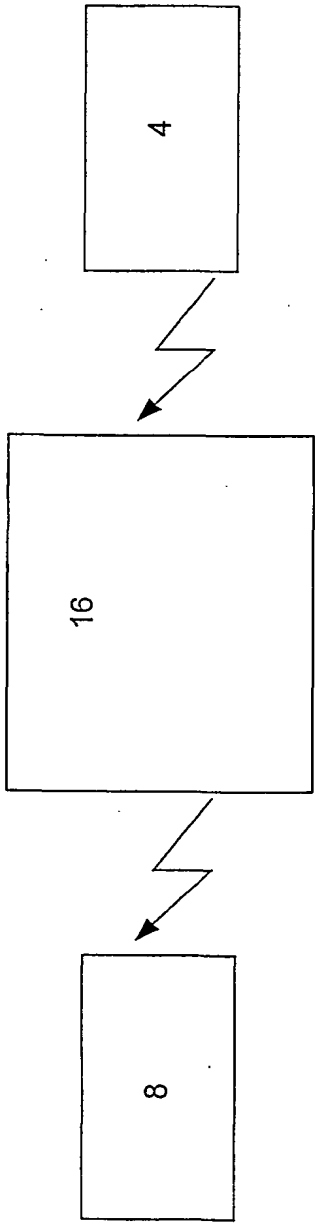


Figure 1

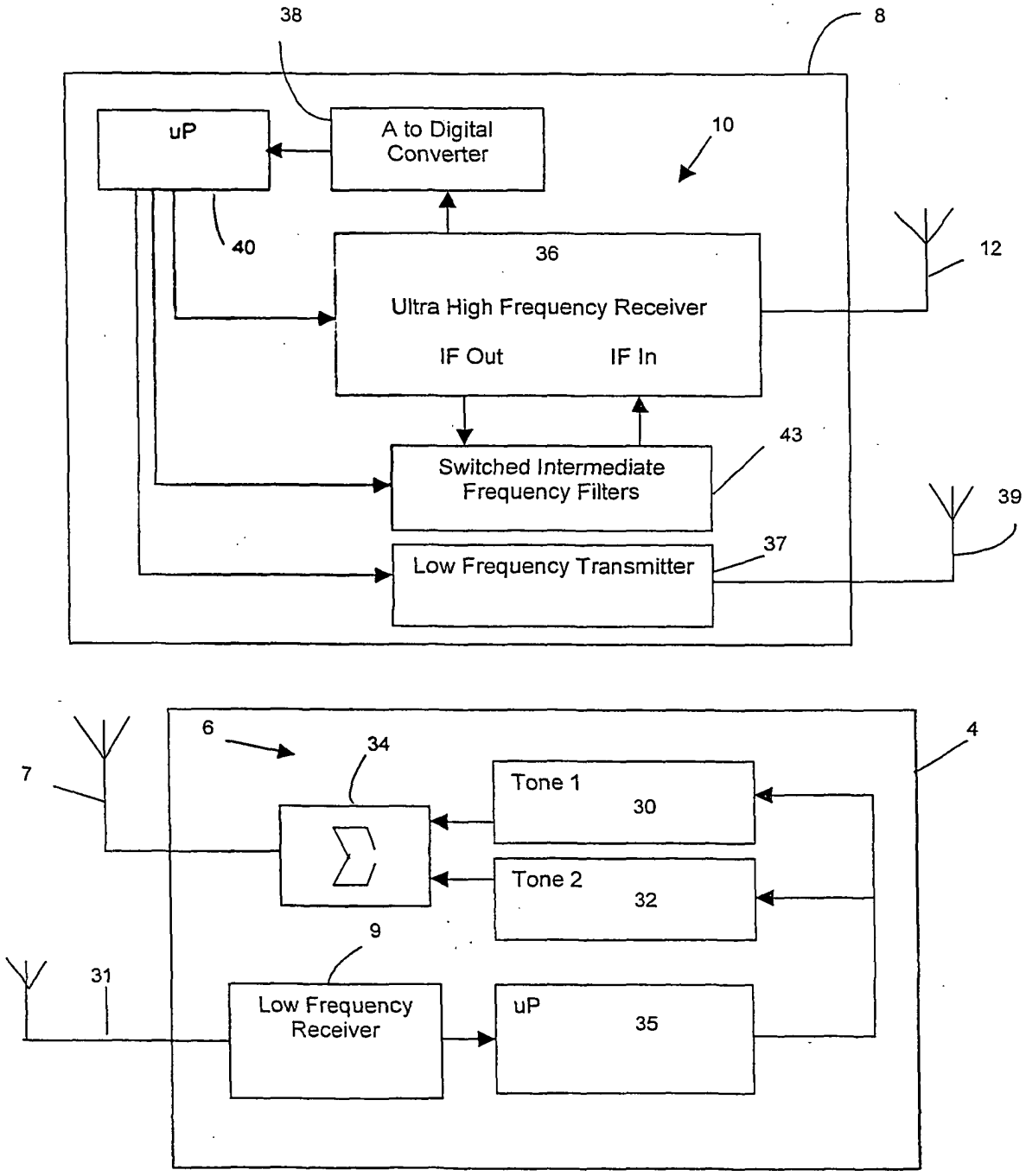


Figure 2

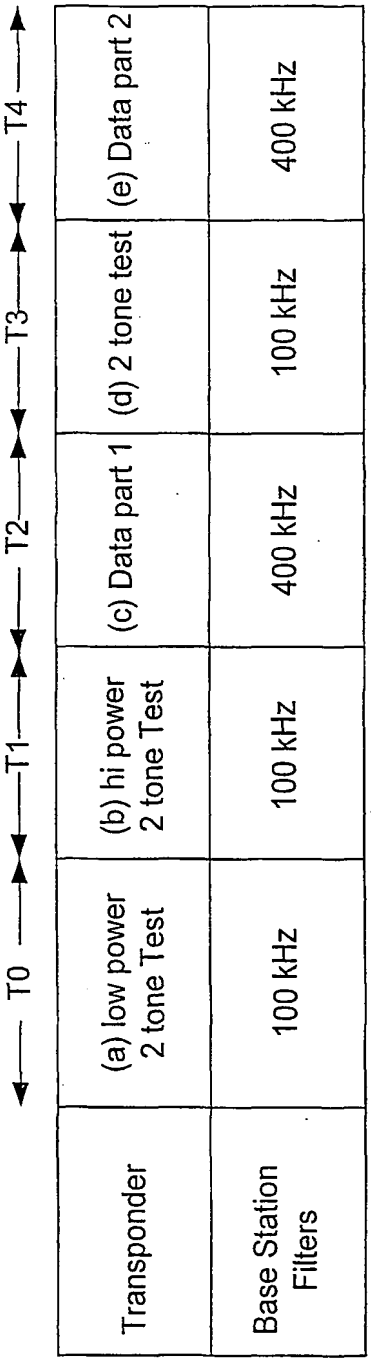


Figure 3

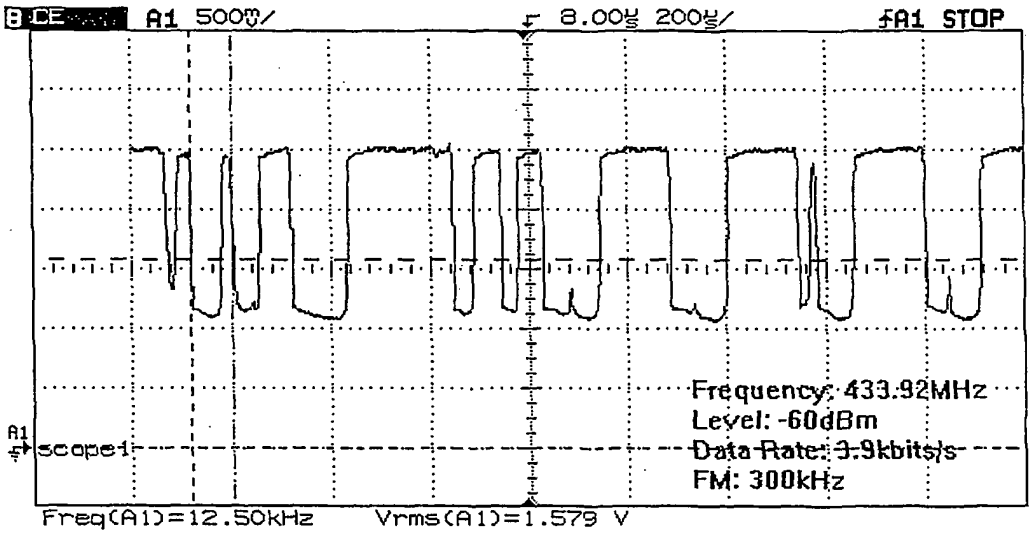


Figure 4

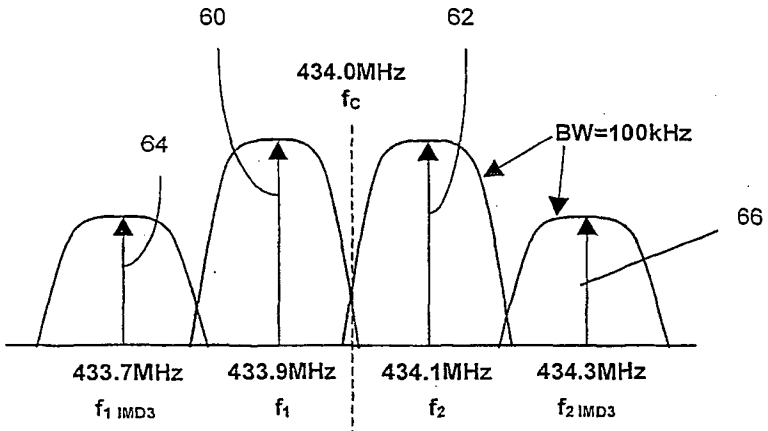


Figure 5

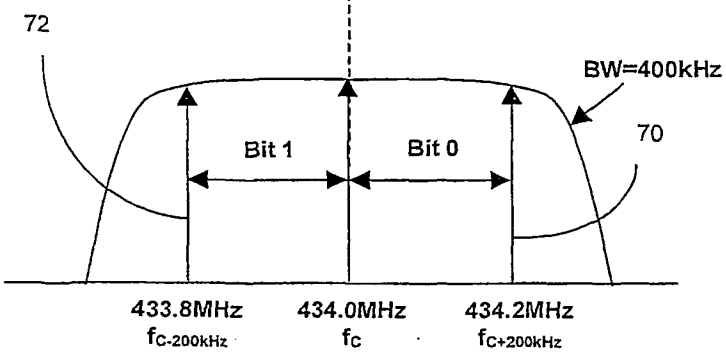


Figure 6

INTERNATIONAL SEARCH REPORT

	al Application No
	PCT/DE 01/02534

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 12848 A (KOSTAL LEOPOLD GMBH & CO KG ;FROMM MICHAEL (DE); KRAMER DETLEV (DE) 9 March 2000 (2000-03-09) abstract; figures 6,7 page 3, line 27 - line 30 page 18, line 11 -page 20, line 4	1,15,16, 19,20, 34,35
X	EP 0 999 103 A (OPEL ADAM AG) 10 May 2000 (2000-05-10) paragraph '0008! - paragraph '0013!	1-5,9, 20-24
A A,P	WO 00 05696 A (PAVATICH GIANFRANCO ;CROWHURST PETER (AU); BOSCH GMBH ROBERT (DE)) 3 February 2000 (2000-02-03) & AU 33933 99 A (BOSCH GMBH ROBERT) 10 February 2000 (2000-02-10) cited in the application	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 2002	04/02/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int[illegible]al Application No
PCT/DE 01/02534

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0012848 A	09-03-2000	DE 19839696 A1	02-03-2000
		DE 19839695 C1	04-05-2000
		DE 19926234 A1	14-12-2000
		AU 5737299 A	21-03-2000
		BR 9913440 A	02-10-2001
		WO 0012848 A1	09-03-2000
		EP 1109981 A1	27-06-2001
EP 0999103 A	10-05-2000	DE 19850792 A1	11-05-2000
		EP 0999103 A2	10-05-2000
WO 0005696 A	03-02-2000	AU 3393399 A	10-02-2000
		BR 9912267 A	17-04-2001
		WO 0005696 A2	03-02-2000
		EP 1099204 A2	16-05-2001

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/DE 01/02534

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 00 12848 A (KOSTAL LEOPOLD GMBH & CO KG ;FROMM MICHAEL (DE); KRAMER DETLEV (DE) 9. März 2000 (2000-03-09) Zusammenfassung; Abbildungen 6,7 Seite 3, Zeile 27 - Zeile 30 Seite 18, Zeile 11 -Seite 20, Zeile 4 ---	1,15,16, 19,20, 34,35
X	EP 0 999 103 A (OPEL ADAM AG) 10. Mai 2000 (2000-05-10) Absatz '0008! - Absatz '0013! ---	1-5,9, 20-24
A	WO 00 05696 A (PAVATICH GIANFRANCO ;CROWHURST PETER (AU); BOSCH GMBH ROBERT (DE)) 3. Februar 2000 (2000-02-03)	
A,P	& AU 33933 99 A (BOSCH GMBH ROBERT) 10. Februar 2000 (2000-02-10) in der Anmeldung erwähnt -----	

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. Januar 2002	04/02/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Buron, E

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

In ales Aktenzeichen
PCT/DE 01/02534

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 0012848	A	09-03-2000	DE	19839696 A1	02-03-2000
			DE	19839695 C1	04-05-2000
			DE	19926234 A1	14-12-2000
			AU	5737299 A	21-03-2000
			BR	9913440 A	02-10-2001
			WO	0012848 A1	09-03-2000
			EP	1109981 A1	27-06-2001
EP 0999103	A	10-05-2000	DE	19850792 A1	11-05-2000
			EP	0999103 A2	10-05-2000
WO 0005696	A	03-02-2000	AU	3393399 A	10-02-2000
			BR	9912267 A	17-04-2001
			WO	0005696 A2	03-02-2000
			EP	1099204 A2	16-05-2001